

**International Conference on Cyber Security
Fordham University
Wednesday, August 4, 2010
9:00 a.m.
McNally Amphitheatre**

**Remarks by
Preet Bharara, U.S. Attorney, Southern District of New York**

Thanks Mark for that kind introduction. Good morning to you all.

I'd like to thank our good friends at the New York Field Office of the FBI and Fordham University for organizing this week's conference, which offers industry and law enforcement the tremendous opportunity to work together to address the ever-evolving cyber crime problem.

The Cyber Crime Threat

I think we all recognize the importance of using every law enforcement tool at our disposal to combat threats to our cyber security. Computer networks – including the biggest one of all, the Internet – are crucial infrastructure supporting our global economy.

We, in the Southern District of New York, are critically aware of this. You need look no further than Wall Street, the nation's vital financial industry, for an obvious illustration of this fact. The securities exchanges, traders and brokers rely heavily – if not exclusively – on computer systems to make billions of dollars worth of transactions each day.

Long gone are the days of paper-strewn trading floors and ticker tape (although as a Yankees fan, I hope there's always enough ticker tape around for the Yankees annual World Series parade down Broadway). Instead, we have automated trading systems residing on computer servers in Manhattan and elsewhere, linked by fiber optic cable to traders around the world who place orders by computer.

While the Internet can often seem like a hazy concept – to some, it's a cloud, and to others, it's like a series of tubes, – in truth it's an enormously complicated physical web of servers, databases, wires and routers that reaches into nearly every home, business, and Government agency in this country.

It provides all of us with instantaneous communication with anyone in the world, nearly limitless applications, and unparalleled convenience and efficiency. And just as the Internet's flexibility and reach has radically transformed the way we communicate and conduct business, its pervasive nature has opened up new avenues for criminals to victimize us – even in our own homes.

The Internet is simultaneously full of promise and fraught with peril.

As I've learned over my last year as the U.S. Attorney, these threats are all too real – from individual phishing emails that trick victims into disclosing personal and financial information; to computer viruses and keystroke loggers that steal victims' passwords to online bank accounts; to the large-scale theft of account information from financial institutions; to denial of service attacks; to the theft of valuable intellectual property over the Internet.

Given what we have seen lately, the laptop and the modem are rapidly replacing the handgun and the ski mask as the preferred tools for robbing a bank.

And as you well know, a cyber attack could have an enormous, if not devastating, impact on our economy. One need only consider a successful denial of service attack on the computer systems used by any of the stock exchanges on Wall Street to get a sense of what would happen.

Cybercrime also has the potential to cripple individual businesses and services. Consider, for example, what happened in January 2010 to Baidu.com, the biggest Internet search engine in China and the third largest in the world.

Hackers using the name "Iranian Cyber Army" took over Baidu's domain name and redirected users to a webpage declaring that the site had been hacked. Baidu alleges that the interruption to its operations cost it millions of dollars in lost revenue and damaged its business reputation. Just last week a judge allowed Baidu.com to proceed with a civil lawsuit against Register.com, the company responsible for maintaining Baidu's domain name.

And Baidu's experience is not unique. A month earlier, in December 2009, the popular micro-blogging site Twitter.com suffered the same attack, preventing millions of Twitter users from accessing their accounts.

Although access to Baidu and Twitter were restored in relatively short amounts of time, these examples demonstrate just one way that cyber crime can instantly harm millions of users.

In monetary terms, cybercrime's impact is no less dramatic. A 2007 report by the Government Accounting Office estimated the direct economic harm from cybercrime to be on the order of \$67 billion dollars, a figure we can all agree has only grown larger since then.

As the amount of money involved in cybercrime has grown, so too has the sophistication and organization of cyber criminals.

We see them becoming specialized, honing their skills in a particular area of expertise. By specializing, cyber criminals can develop a reputation, establish steady client relationships with multiple criminal partners, focus their time and energy on improving their goods and services, and increase their profit potential.

These specializations include coders, who create the malicious programs that are necessary to steal valuable data like bank account information; vendors, who trade and sell the stolen data; cashers, or money mules, often unsophisticated individuals who use the information to illegally withdraw cash from compromised accounts; and money launderers, who often hide the criminal origin of the illicit proceeds by converting it into digital currency.

We also see today's professional cyber criminals using their own underground social networking sites to communicate, organize, and scheme together.

Just like the old-world social clubs used by La Cosa Nostra – the traditional mafia, in the cases I used to prosecute as a new AUSA in the Southern District -- these hidden Internet forums are exclusive and invitation-only.

New members must be vouched for by existing members. But once on the inside, cyber criminals can easily make new contacts, buy, sell or trade contraband, and keep up-to-date on the latest crime techniques.

To be sure, there are some obvious yet crucial differences between traditional organized crime and the new breed of cyber criminals.

Just as the Internet has increased the efficiency of communication and commerce, it has also allowed cyber criminals anywhere in the world to work together easily without respect for jurisdictions or national boundaries, rather than a more restricted geographic area like New York City's notorious mafia families.

And, while Mafia members and cyber criminal each get to choose their own nicknames – although you're not liable to find too many "Fat Tonys" or "Little Larrys" in cyberspace – the Internet allows cyber criminals to operate with something of which old school mobsters can only dream of -- near-complete anonymity behind their instant messaging account number or nickname.

Cyber criminals don't need to resort to the old-fashioned walk and talk.

So it goes almost without saying that the investigation and prosecution of cyber crime represents the absolute cutting edge of criminal law enforcement.

Given the unique challenges presented by this type of crime, I am glad that we have the best minds in Government and industry working on this problem – and meeting here this week.

You will be hearing directly from Director Mueller tomorrow, but let me say that there is no one in America who better understands – and has more urgently emphasized – the need for cyber security: to protect our citizens, our economy, and our homeland.

Here in New York, we're lucky to be able to work with the FBI, which is at the absolute vanguard of the emerging fight against cyber crime.

The FBI's New York Office is the largest in the country, and, recognizing the critical threat to us all from computer crime, it's greatly increased the resources devoted to the problem.

Most impressively, FBI New York has stood up an entire cyber crime branch, headed by some of the most experienced agents around – Special Agent in Charge Mary Galligan and acting Assistant Special Agent in Charge Austin Berglas.

Within the branch are specialized units to address cyber terrorism, computer intrusions, and fraud committed over the Internet. They are led by Supervisory Special Agents Bete Santos, Chris Stangl, and Peter Grossgold. They are here and you should make it a point to meet them.

My office works closely with our colleagues at the FBI to address the cyber crime threat. But we can't do it alone. That is why this conference is especially important because coordination between law enforcement and industry is often the key to solving cyber crime cases.

What We Are Doing to Fight Cyber Crime

But before I talk about how and **why** we should work together, I want to give you a sense of some of the work that the Assistant U.S. Attorneys in my office – the federal prosecutors in the Southern District of New York – have been doing to combat cyber crime. In case it's not already clear to you from what I've been saying, I place a high priority on prosecuting cyber criminals.

As a result, one of the first changes I made to my office after I was confirmed as U.S. Attorney was to create the Complex Frauds Unit, whose mission is to handle the prosecution of cyber crimes and other sophisticated fraud schemes. Jonathan Kolodner and Anirudh Bansal, who are here today, head up the Complex Frauds Unit.

Assigned to that unit are a number of prosecutors who have received special training in the nuances and difficulties of cybercrime investigations and prosecutions. These AUSAs are led by Tom Brown, the office's cyber crime coordinator, who is also here today. But not just these AUSAs work on cyber crime.

All of the twenty prosecutors in the Complex Frauds Unit make it a priority to build cyber crime cases. And it's not just the Complex Frauds Unit that is handling these matters – cyber crime cases are being worked on across the office – in the organized crime unit, the terrorism unit, and even by junior AUSAs. So as we shine a spotlight on these offenses, my office is committed to expanding our cyber crime prosecutions.

A significant part of my office's cyber crime strategy has been to develop and strengthen our relationships with foreign prosecutors and law enforcement agencies to target cyber criminals wherever they are found and to put them on notice that they are at risk of prosecution, no matter how safe they think they are. Cyber criminals work effortlessly across borders; that means we have to do the same.

As I've mentioned, the Internet's unique ability to connect people globally has made cyber crime one of the most international of criminal activities. And all too often, while international borders are obstacles to effective law enforcement, criminals see these boundaries as opportunities to confound prosecution.

My office recognizes that close coordination among international law enforcement partners is crucial to overcoming the transnational challenge posed by cyber crime and to eliminate any safe havens for cyber criminals.

As a result, over the last two years the Southern District has worked on investigations with a number of foreign partners, including Estonia, Romania, the Ukraine, Belarus, Lithuania, the Netherlands, the U.K., the Czech Republic, and the Dominican Republic. Many of these investigations are ongoing. Representatives from most of these countries are here this week, and I know prosecutors from my office will be meeting with them to advance our mutual cases.

Significant Cases

Working with our law enforcement partners in the United States and abroad, we have had a string of successes in the war on cybercrime.

Let me mention a few to give you a sense of where we are, where we are going, and what is possible:

A recent example of this office's international pursuit of cyber criminals is prosecution of Dmitry Naskovets, a Belarusian. Naskovets, together with a fellow national, Sergey Semashko, operated CallService.biz, as an illegal service for online identity thieves.

As you know, many financial institutions and Internet-based business have in place security measures to verify the identity of customers who wish to make transfers or withdrawals from bank accounts or make purchases with credit cards over the Internet.

Among other things, customers may be required to confirm their identity to service representatives over the telephone.

To beat this security measure, Naskovets and Semashko would provide the services of English- and German-speaking individuals to online identity thieves. The English and German speakers, using stolen account and biographic information supplied by the identity thieves, would pose as authorized account holders and confirm fraudulent transactions over the telephone.

According to advertisements for CallService.biz on underground Internet forums used by identity thieves, the CallService.biz website had performed over 5400 confirmation calls to banks.

In April of this year, the Southern District of New York and the FBI, together with the Czech Republic, Belarus, and Lithuania, conducted a coordinated international takedown of CallService.biz's illegal business.

- Czech police arrested Naskovets in Prague, where he was living.
- Simultaneously, law enforcement in Belarus arrested Semashko.
- And Lithuanian law enforcement seized the computers on which the CallService.biz website was hosted.
- At the same time, the FBI in New York seized the CallService.biz domain name. Rather than just take down the domain name, however, the FBI put up a banner announcing the seizure.

If you care to see the banner -- and I would encourage you to do so -- just type C-A-L-L-S-E-R-V-I-C-E-DOT-B-I-Z into your web browser. Don't worry -- I promise it's safe.

I can tell you that the seizure banner, which is what online identity thieves who thought they were visiting the CallService.biz website now see, has caused considerable anxiety in the online criminal world, enhancing the deterrent effect of the arrests of Naskovets and Semashko.

Indeed, we have since used domain name seizures and banners to similar effect with another law enforcement partner, Immigration and Customs Enforcement in an Operation called "In Our Sites," which targeted websites that distributed illegal copies of movies, music, games, software and television shows over the Internet.

On June 30 of this year, we seized seven domain names -- with names such as TVShack.net and ThePirateCity.org that don't exactly hide what these sites are doing -- and replaced them with seizure banners. In the weeks that followed, several other websites that distributed infringing contents have unilaterally stopped doing so. We believe that was in part because of the tremendous amount of attention that the banners attracted online. That is another heartening example of the power of deterrence in this area.

Here's another example: This office is also prosecuting Ilya Boruch, who ran a company called Bidding Expert in Queens, New York.

On his website, Boruch claimed to offer various financial services to his customers, including converting cash into WebMoney, so-called digital currency that can be sent anonymously over the Internet.

Boruch is alleged to have taken more than a million dollars in cash from two individuals

who were part of a conspiracy to fraudulently withdraw money from ATMs in New York City using stolen account information that they received from another criminal over the Internet. According to charging documents in the case, Boruch would meet the two individuals on the street in Queens and Brooklyn, where they would literally hand him bags of money.

After receiving the cash, Boruch is alleged to have laundered it by converting it into WebMoney for his fraudster clients, who sent it to their co-conspirator overseas. A trial for Boruch is pending.

We also worked cooperatively with the Dominican National Police to dismantle a ring of identity thieves operating from the Dominican Republic. Participants in this transnational conspiracy were filing thousands of fraudulent federal income tax refund claims using identities stolen from residents of Puerto Rico. And they were filing all of these returns with the U.S. taxation authority electronically, from computers in homes and apartments scattered throughout an area of the Dominican Republic, believing that they were safe from law enforcement.

Together with our partners in the Dominican Republic, during the first few weeks of 2009 we tracked these criminals over the Internet by their IP addresses as they filed over 8,000 tax returns seeking over \$90 million worth of fraudulent refunds.

In late February 2009, together with Dominican law enforcement we conducted simultaneous arrests of a total of 14 individuals here in New York City and in the Dominican Republic.

These are just a few examples of the cybercrime cases that the Southern District has been doing.

Together they show that collaboration is vital, prosecution is possible, and deterrence is achievable.

Private Sector Collaboration

As I said before, cybercrime cases require collaboration, not only among law enforcement agencies, but also between the government and industry. Victim companies are on the front lines of this battle, and are often the first to realize that a cyber attack has taken place. Unless we know about the problem, our ability to help is limited. That is why our private sector partnerships are so important.

We understand that there has traditionally been a dichotomy between businesses wishing to maintain the security of their networks and law enforcement investigations.

Business may feel that they lose control of the process, and that confidential business information could be exposed. Companies might even think that reporting a breach may harm their competitive advantage.

But businesses should know that we will do everything that we can to minimize disruptions to their operations, and to safeguard confidential data. Where necessary, we will seek protective orders – orders signed by a federal judge that help to preserve trade secrets and business confidentiality. And we will share with victim companies what we can, as fast as we can, about a particular attack.

The private sector, particularly international companies, are on the front-lines of this fight. Many of them have know-your-customer policies and anti-fraud systems, which not only keep out unwanted intruders and prevent criminals from making use of legitimate business channels, but give advance warning of where the next cyber crime wave will be coming from.

At the end of the day, we can and must help each other, by maintaining clear lines of communication between law enforcement and the businesses that are affected by cyber crime.

Closing

Cybercrime respects no boundaries. It presents a grave threat to this country, and its perpetrators are constantly honing their attacks. No one country, no one agency, no one company can alone stop cyber attacks. It is only together that we can minimize this law enforcement and national security challenge. We have had great success prosecuting cyber criminals so far, and I know that by working together we will continue and expand on this success.

Given what is at stake for our economy and our security, we have no choice.

Please enjoy the rest of the conference.

Thank you.